Interactive Advertising Bureau & Tech Lab
116 East 27th Street, 7th Floor
New York, New York 10016

4 September 2018

Dear colleague,

Re: feedback on the beta OpenRTB 3.0 specification

The IAB has requested input on the beta OpenRTB 3.0 specification. This response sets out an acute concern about the lack of data protection in this specification.

The protection of personal data has been absent from previous OpenRTB specifications. It is a matter of concern to Internet users, and is also now of utmost commercial concern to marketers. This commercial concern arises from two facts.

First, as you will no doubt know, a recent ruling at the European Court of Justice, on 5 June (C-210/16), indicates that marketers are directly exposed as "controllers" to legal risk from data protection infringements in data processing that they commission, or cause to be commissioned. The Court ruled that this applies even if the marketer never directly handles the personal data.

Second, under Article 82 (4) of the General Data Protection Regulation, a marketer may be exposed to the "entire damage" created by ad tech vendors that process personal data in the OpenRTB system, which infringes the Regulation. In other words, marketers are now liable for the misuse of personal data in the RTB system.

OpenRTB 3.0, and previous iterations of OpenRTB, causes an acute data protection problem. Every time a person loads a page on a website that uses OpenRTB 3.0 advertising, personal data about them are broadcast to tens - or hundreds - of companies in the OpenRTB bid request. These personal data include:[1]

- Your IP address
- What you are reading or watching
- Your location
- Description of your device, and ad tech companies' unique IDs for you. (This will allow ad tech companies to try to reidentify you the next time you are seen, so that a long-term profile can be built or consolidated with offline data about you.)
- Data broker segment ID, if available. (This could denote things like your income bracket, age and gender, habits, social media influence, ethnicity, sexual orientation, religion, political leaning, etc.)[2]

[1] "AdCOM Specification v1.0, Beta Draft", IAB TechLab, 24 July 2018.
[2] See "Object: data" and "Object: segment" in ibid.

These data are very likely to include "special categories"[3] of personal data, since they show what the person is watching and reading, and since the OpenRTB 3.0 specification enables the inclusion of data brokers' segment IDs.[4]

A more complete summary of the personal data in bid requests is provided for your convenience in Appendix 1. Relevant excerpts from the OpenRTB AdCOM specification are provided in Appendix 2.

The broadcast of these personal data under OpenRTB is referred to as an "RTB bid request". As with previous iterations of OpenRTB, this will be generally broadcast widely, since the objective is to solicit bids from companies that might want to show an ad to the person who has just loaded the webpage. An RTB bid request is broadcast on behalf of websites by companies known as "supply side platforms" (SSPs) and by "ad exchanges".

Personal data are broadcast in bid requests to multiple Demand Side Partners (DSPs), which then decide whether to place bids for the opportunity to show an ad to the person in question. The DSP acts on behalf of a marketer, and decides when to bid based on the profile of person that the marketer has instructed it to target. Sometimes, Data Management Platforms (DMPs), of which Cambridge Analytica is a notorious example, can perform a sync that contributes to their existing profiles of the person. It is worth noting that this sync would not be possible without the initial bid request.

RTB as presented in the OpenRTB 3.0 specification is a data protection free zone.

The overriding commercial incentive for many ad tech companies is to share as many data with as many partners as possible, and to share it with partner or parent companies that run data brokerages. Clearly, releasing personal data into such an environment has high risk.

Despite this high risk, the OpenRTB 3.0 specification establishes no control over what happens to these personal data once an SSP or ad exchange broadcasts a "bid request". Even if bid request traffic is secure, there are no technical measures that prevent the recipient of a bid request from, for example, combining them with other data to create a profile, or from selling the data on. In other words, there is no data protection.

I note that IAB Europe's own documentation on how such a broadcast of personal data could conform with European data protection law reveals the industry view: A company "<u>may choose</u> not to pass bid requests containing personal data to

[3] "…revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation…", in the General Data Protection Regulation, Article 9 (1).

[4] "Object: data" and "Object: segment" in "AdCOM Specification v1.0, Beta Draft", IAB TechLab, 24 July 2018.

other vendors who do not have consent".[5] In other words, once DSPs receive personal data they can freely trade these personal data with business partners however they wish. The distribution of a bid request creates this data protection-free zone.

In fact, this is very likely to be a data breach. The RTB bid request, including the data specified in the OpenRTB 3.0 specification, fits within the General Data Protection Regulation's definition of "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".[6]

This is particularly egregious since the data concerned are very likely to be "special categories" of personal data, and since I believe that the industry concerned is aware of the shortcomings of this approach, and has continued to pursue it regardless.

In summary, the OpenRTB 3.0 specification will continue to leak details about what every person is reading or watching in a constant broadcast to a large number of companies. These personal data are not protected. This breach is continuous, happening on virtually every website, every single time a person loads a page.

Unless OpenRTB 3.0 is very radically altered, so that no personal data are contained in the bid request, it appears that it will be a severe infringement of Article 5 of the General Data Protection Regulation, and on all that flows from Article 5's principles. This will put at risk the fundamental rights of virtually every person that uses the Internet in Europe. These rights are enshrined in and protected by the Charter of Fundamental Rights of the European Union. As a result, marketers, vendors, and publishers will be exposed to acute legal hazard.

We must therefore urge that you reconsider the OpenRTB 3.0 specification. So long as the bid request is permitted to contain personal data, and so long as these personal data are widely shared, OpenRTB will be a liability. The RTB system must not be allowed to continue as a data protection "wild west".

Yours faithfully,

Dr Johnny Ryan FRHistS
Chief Policy & Industry Relations Officer
Brave

[5] "Transparency & Consent Framework, FAQ", IAB Europe, 16 April 2018, p. 11.
[6] GDPR, Article 4, paragraph 12.

Appendix 1. What personal data are shared in RTB bid requests?

This summary list is incomplete. Other fields that can contain personal data.[7]

"Site"[8]

- The specific URL that a visitor is loading, which shows what they are reading or watching.

"Device"[9]

- Operating system and version.
- Browser software and version.
- IP address.
- Device manufacturer, model, and version.
- Height of the screen.
- Width of the screen.
- Screen ratio.
- Whether JavaScript is supported.
- The version of Flash supported by the browser.
- Language settings.
- Carrier / ISP.
- Type of connection, if mobile.
- Network connection type.
- Hardware device ID (hashed).
- MAC address of the device (hashed).

"User"[10]

- An Ad Exchange's unique personal identifier for the visitor to the website. (This may rotate, but the specification says that it "must be stable long enough to serve reasonably as the basis for frequency capping and retargeting."[11])
- Advertiser's "buyeruid", a unique personal identifier for the data subject.
- The website visitor's year of birth, if known.
- The website visitor's gender, if known.
- The website visitor's interests.
- Additional data about the website visitor, if available from a data broker.[12] (These may include the "segment"[13] category previously decided by the data broker, based on the broker's previous profiling of this particular person.)

"Geo"[14]

- Location latitude and longitude.
- Zip/postal code.

---

[7] For example, thirty eight of the data fields in the specification contain the phrase "optional vendor specific extensions".

[8] "Object: site" in "AdCOM Specification v1.0, Beta Draft", IAB TechLab, 24 July 2018.

[9] "Object: device" in ibid.

[10] "Object: device" in ibid.

[11] ibid.

[12] "Object: data" in ibid.

[13] "Object: segment" in ibid.

[14] "Object: device" in ibid.

Appendix 2. Selected data tables from IAB specification documents

The following tables are copied from AdCOM specification v1, which is part of the OpenRTB 3.0 specification.[15] Only selected tables relevant to website bid requests are included here. URLs of the specific part of the specification from where the tables are taken are presented above each table.

Object: Site

Derived from: DistributionChannel

This object is used to define an ad supported website, in contrast to a non-browser application, for example. As a derived class, a "Site" object inherits all "DistributionChannel" attributes and adds those defined below.

Attribute	Type	Definition
domain	string	Domain of the site (e.g., "mysite.foo.com").
cat	string array	Array of content categories describing the site using IDs from the taxonomy indicated in "cattax".
sectcat	string array	Array of content categories describing the current section of the site using IDs from the taxonomy indicated in "cattax".
pagecat	string array	Array of content categories describing the current page or view of the site using IDs from the taxonomy indicated in "cattax".
cattax	integer	The taxonomy in use for the "cat", "sectcat" and "pagecat" attributes. Refer to List: Category Taxonomies.
privpolicy	integer	Indicates if the site has a privacy policy, where 0 = no, 1 = yes.
keywords	string	Comma separated list of keywords about the site.
page	string	URL of the page within the site.
ref	string	Referrer URL that caused navigation to the current page.
search	string	Search string that caused navigation to the current page.
mobile	integer	Indicates if the site has been programmed to optimize layout when viewed on mobile devices, where 0 = no, 1 = yes.
amp	integer	Indicates if the page is built with AMP HTML, where 0 = no, 1 = yes.
ext	object	Optional vendor-specific extensions.

https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20BETA%201.0.md#object--site-

[15] "AdCOM Specification v1.0, Beta Draft", IAB TechLab, 24 July 2018 (URL: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20BETA%201.0.md).

Object: Publisher

This object describes the publisher of the media in which ads will be displayed.

Attribute	Type	Definition
id	string, recommended	Vendor-specific unique publisher identifier, as used in ads.txt files.
name	string	Displayable name of the publisher.
domain	string	Highest level domain of the publisher (e.g., "publisher.com").
cat	string array	Array of content categories that describe the publisher using IDs from the taxonomy indicated in "cattax".
cattax	integer	The taxonomy in use for the "cat" attribute. Refer to List: Category Taxonomies.
ext	object	Optional vendor-specific extensions.

https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20BETA%201.0.md#object--publisher-

Object: User

This object contains information known or derived about the human user of the device (i.e., the audience for advertising). The user ID is a vendor-specific artifact and may be subject to rotation or other privacy policies. However, this user ID must be stable long enough to serve reasonably as the basis for frequency capping and retargeting.

Attribute	Type	Definition
id	string; recommended	Vendor-specific ID for the user. At least one of "id" or "buyeruid" is strongly recommended.
buyeruid	string; recommended	Buyer-specific ID for the user as mapped by an exchange for the buyer. At least one of "id" or "buyeruid" is strongly recommended.
yob	integer	Year of birth as a 4-digit integer.
gender	string	Gender, where "M" = male, "F" = female, "O" = known to be other (i.e., omitted is unknown).
keywords	string	Comma separated list of keywords, interests, or intent.
consent	string	GDPR consent string if applicable, complying with the comply with the IAB standard Consent String Format in the Transparency and Consent Framework technical specifications.
geo	object	Location of the user's home base (i.e., not necessarily their current location). Refer to Object: Geo.
data	object array	Additional user data. Each "Data" object represents a different data source. Refer to Object: Data.
ext	object	Optional vendor-specific extensions.

https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20BETA%201.0.md#object--user-

Object: Device

This object provides information pertaining to the device through which the user is interacting. Device information includes its hardware, platform, location, and carrier data. The device can refer to a mobile handset, a desktop computer, set top box, or other digital device.

Attribute	Type	Definition
type	integer	The general type of device. Refer to List: Device Types.
ua	string	Browser user agent string.
ifa	string	ID sanctioned for advertiser use in the clear (i.e., not hashed).
dnt	integer	Standard "Do Not Track" flag as set in the header by the browser, where 0 = tracking is unrestricted, 1 = do not track.
lmt	integer	"Limit Ad Tracking" signal commercially endorsed (e.g., iOS, Android), where 0 = tracking is unrestricted, 1 = tracking must be limited per commercial guidelines.
make	string	Device make (e.g., "Apple").
model	string	Device model (e.g., "iPhone").
os	integer	Device operating system. Refer to List: Operating Systems.
osv	string	Device operating system version (e.g., "3.1.2").
hwv	string	Hardware version of the device (e.g., "5S" for iPhone 5S).
h	integer	Physical height of the screen in pixels.
w	integer	Physical width of the screen in pixels.
ppi	integer	Screen size as pixels per linear inch.
pxratio	float	The ratio of physical pixels to device independent pixels.
js	integer	Support for JavaScript, where 0 = no, 1 = yes.
lang	string	Browser language using ISO-639-1-alpha-2.
ip	string	IPv4 address closest to device.
ipv6	string	IP address closest to device as IPv6.
xff	string	The value of the x-forwarded-for header.
iptr	integer	Indicator of truncation of any of the IP attributes (i.e., "ip", "ipv6", "xff"), where 0 = no, 1 = yes (e.g., from 1.2.3.4 to 1.2.3.0). Refer to tools.ietf.org/html/rfc6235#section-4.1.1 for more information on IP truncation.
carrier	string	Carrier or ISP (e.g., "VERIZON") using exchange curated string names which should be published to bidders a priori.
mccmnc	string	Mobile carrier as the concatenated MCC-MNC code (e.g., "310-005" identifies Verizon Wireless CDMA in the USA). Refer to en.wikipedia.org/wiki/Mobile_country_code for further information and references. Note that the dash between the MCC and MNC parts is required to remove parsing ambiguity.
mccmncsim	string	MCC and MNC of the SIM card using the same format as "mccmnc". When both values are available, a difference between them reveals that a user is roaming.
contype	integer	Network connection type. Refer to List: Connection Types.
geofetch	integer	Indicates if the geolocation API will be available to JavaScript code running in display ad,

geofetch	integer	Indicates if the geolocation API will be available to JavaScript code running in display ad, where 0 = no, 1 = yes.
geo	object	Location of the device (i.e., typically the user's current location). Refer to Object: Geo.
ext	object	Optional vendor-specific extensions.

https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20BETA%201.0.md#object--device-

Object: Geo

This object encapsulates various methods for specifying a geographic location. When subordinate to a "Device" object, it indicates the location of the device which can also be interpreted as the user's current location. When subordinate to a "User" object, it indicates the location of the user's home base (i.e., not necessarily their current location).

The "lat" and "lon" attributes should only be passed if they conform to the accuracy depicted in the "type" attribute. For example, the centroid of a large region (e.g., postal code) should not be passed.

Attribute	Type	Definition
type	integer	Source of location data; recommended when passing lat/lon. Refer to List: Location Types.
lat	float	Latitude from -90.0 to +90.0, where negative is south.
lon	float	Longitude from -180.0 to +180.0, where negative is west.
accur	integer	Estimated location accuracy in meters; recommended when lat/lon are specified and derived from a device's location services (i.e., type = 1). Note that this is the accuracy as reported from the device. Consult OS specific documentation (e.g., Android, iOS) for exact interpretation.
lastfix	integer	Number of seconds since this geolocation fix was established. Note that devices may cache location data across multiple fetches. Ideally, this value should be from the time the actual fix was taken.
ipserv	integer	Service or provider used to determine geolocation from IP address if applicable (i.e., "type" = 2). Refer to List: IP Location Services.
country	string	Country code using ISO-3166-1-alpha-2. Note that alpha-3 codes may be encountered and vendors are encouraged to be tolerant of them.
region	string	Region code using ISO-3166-2; 2-letter state code if USA.
metro	string	Regional marketing areas such as Nielsen's DMA codes or other similar taxonomy to be agreed among vendors prior to use. Note that DMA is a trademarked asset of The Nielsen Company. Vendors are encouraged to ensure their use of DMAs is properly licensed.
city	string	City using United Nations Code for Trade & Transport Locations "UN/LOCODE" with the space between country and city suppressed (e.g., Boston MA, USA = "USBOS"). Refer to UN/LOCODE Code List.
zip	string	ZIP or postal code.
utcoffset	integer	Local time as the number +/- of minutes from UTC.
ext	object	Optional vendor-specific extensions.

https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20BETA%201.0.md#object--geo-

Object: Data

The data and segment objects together allow additional data about the related object (e.g., user, content) to be specified. This data may be from multiple sources whether from the exchange itself or third parties as specified by the "id" attribute. When in use, vendor-specific IDs should be communicated *a priori* among the parties.

Attribute	Type	Definition
id	string	Vendor-specific ID for the data provider.
name	string	Vendor-specific displayable name for the data provider.
segment	object array	Array of "Segment" objects that contain the actual data values. Refer to Object: Segment.
ext	object	Optional vendor-specific extensions.

https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20BETA%201.0.md#object--data-

Object: Segment

Segment objects are essentially key-value pairs that convey specific units of data. The parent "Data" object is a collection of such values from a given data provider. When in use, vendor-specific IDs should be communicated *a priori* among the parties.

Attribute	Type	Definition
id	string	ID of the data segment specific to the data provider.
name	string	Displayable name of the data segment specific to the data provider.
value	string	String representation of the data segment value.
ext	object	Optional vendor-specific extensions.

https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20BETA%201.0.md#object--segment-